JAY EDELSON (Admitted *Pro Hac Vice*)
(jedelson@edelson.com)
RAFEY S. BALABANIAN (Admitted *Pro Hac Vice*)
(rbalabanian@edelson.com)
ARI J. SCHARG (Admitted *Pro Hac Vice*)
(ascharg@edelson.com)
CHRISTOPHER L. DORE (Admitted *Pro Hac Vice*)
(cdore@edelson.com)
EDELSON MCGUIRE, LLC
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Tel: (312) 589-6370

LAURENCE D. KING (SBN 206423)
(lking@kaplanfox.com)
LINDA M. FONG (SBN 124232)
(lfong@kaplanfox.com)
KAPLAN FOX & KILSHEIMER LLP
350 Sansome Street, Suite 400
San Francisco, California 94104
Tel: (415) 772-4700

[Additional counsel appear on the signature page.]

Counsel for Plaintiffs and the Putative Class and Subclass

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

IN RE LINKEDIN USER PRIVACY LITIGATION

Case No. 12-cv-03088-EJD

FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT FOR:

(1) Violations of Cal. Bus. & Prof. Code §§ 17200, *et seq.*;
(2) Breach of Contract;
(3) Restitution/Unjust Enrichment;
(4) Breach of the Implied Covenant of Good Faith and Fair Dealing;
(5) Breach of Implied Contracts;
(6) Negligence; and
(7) Negligence *Per Se*.

DEMAND FOR JURY TRIAL

Plaintiffs Katie Szpyrka ("Szpyrka") and Khalilah Wright ("Wright") (collectively, "Plaintiffs"), by and through their attorneys, upon personal knowledge as to themselves and their own acts and experiences, and upon information and belief as to all other matters, allege as follows:

NATURE OF THE ACTION

1. Plaintiffs Szpyrka and Wright bring this First Amended Consolidated Class Action Complaint ("Complaint") against Defendant LinkedIn Corporation ("Defendant" or "LinkedIn") for failing to properly safeguard its users' digitally stored personally identifiable information ("PII"), including their login credentials.

2. LinkedIn is an Internet company that owns and operates the website www.LinkedIn.com—a social networking website with over 120 million registered users worldwide.

3. Through its Privacy Policy, LinkedIn promises its users that "[a]ll information that [they] provide [to LinkedIn] will be protected with industry standard protocols and technology."[1] In direct contradiction to this promise, however, LinkedIn failed to comply with basic industry standards by maintaining millions of users' PII on its servers in a weak encryption format, and without implementing other crucial security measures.

4. Sometime this year, hackers infiltrated LinkedIn's servers and accessed the database(s) containing its users' PII. After retrieving this data, the hackers publicly posted over 6 million LinkedIn users' passwords online. Because LinkedIn used insufficient encryption methods to secure the user data, hackers were able to easily decipher a large number of the passwords.

5. While some security threats are unavoidable in a rapidly developing technological environment, LinkedIn's failure to comply with long standing industry standard encryption

[1] LinkedIn "Privacy Policy," http://www.linkedin.com/static?key=privacy_policy&trk=hb_ft_priv (last visited November 26, 2012).

protocols jeopardized its users' PII, and diminished the value of the services provided by Defendant—as guaranteed by its own contractual terms.

PARTIES

6. Plaintiff Katie Szpyrka is a natural person and resident of the State of Illinois. Plaintiff Szpyrka is a registered user of LinkedIn's services.

7. Plaintiff Khalilah Wright is a natural person and resident of the State of Virginia. Plaintiff Khalilah is a registered user of LinkedIn's services.

8. Defendant LinkedIn Corporation is a corporation incorporated in and existing under the laws of the State of Delaware, with its principal place of business located at 2029 Stierlin Court, Mountain View, California 94043. LinkedIn does business throughout this District, the State of California, and the United States.

JURISDICTION AND VENUE

9. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), because (a) at least one member of the putative class is a citizen of a state different from Defendant, (b) the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and (c) none of the exceptions under the subsection apply to this action.

10. This Court has personal jurisdiction over Defendant because it is headquartered in this District, conducts significant business in this District, and the unlawful conduct alleged in the Complaint occurred in, was directed to, and/or emanated from this District.

11. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant maintains its headquarters and principal place of business in this District and a substantial part of the events giving rise to Plaintiffs' Complaint occurred in this District.

FACTUAL BACKGROUND

12. LinkedIn's website states that it "operates the world's largest professional network on the Internet with more than 120 million members in over 200 countries and territories [and] represents a valuable demographic for marketers with an affluent & influential

membership."[2]

13. A customer may sign up for a membership at www.LinkedIn.com by providing Defendant with a valid e-mail address and a registration password. LinkedIn then stores these credentials in databases located on its servers. Once registered, users build personal "profiles" by providing LinkedIn with various types of demographic, occupational, and cultural information, including employment and educational history.

14. Defendant offers users the ability to upgrade to a paid "premium" account, with prices ranging from $19.95 to $99.95 per month.

15. In signing up for a premium account, LinkedIn asserts through its Privacy Policy that it will safeguard its users' sensitive PII, specifically that: "All information that you provide will be protected with industry standard protocols and technology." Plaintiffs and members of the Class agreed to LinkedIn's User Agreement and Privacy Policy in order to register and use LinkedIn's services.

16. Importantly, when signing up for and purchasing a "premium" account, Plaintiffs and the members of the Class relied on LinkedIn's representation that it uses "industry standard protocols and technology" to preserve the integrity and security of their personal information in agreeing to create an account and provide their PII to the company.

LinkedIn Fails to Properly Encrypt its Users' PII

17. As discussed above, LinkedIn digitally stores millions of users' PII in a large-scale commercial database on its servers, and affirmatively represents and promises through its Privacy Policy that it uses "industry standard protocols and technology" to protect such PII.

18. However, and despite its contractual obligation to use best practices in storing user data, LinkedIn failed to utilize basic industry standard encryption methods. In particular, LinkedIn failed to adequately protect user data because it stored passwords in unsalted SHA-1

[2] LinkedIn "About Us," http://press.linkedin.com/about (last visited November 26, 2012).

hashed[3] format. The problem with this practice is two-fold. First, SHA-1 is an outdated hashing function, first published by the National Security Agency in 1995. Secondly, storing users' passwords in hashed format without first "salting" the password runs afoul of conventional data protection methods, and poses significant risks to the integrity of users' sensitive data.

19. Industry standards require *at least* the additional process of adding "salt" to a password before running it through a hashing function—a process whereby random values are combined with a password before the text is input into a hashing function. This procedure drastically increases the difficulty of deciphering the resulting encrypted password.

20. The more common industry practice is to (1) salt passwords before inputting them into a hash function, (2) salt the resulting hash value, and (3) then again run the hash value through a hashing function. Finally, that fully encrypted password is stored on a separate and secure server apart from all other user information. Defendant's data protection procedures fell well short of this level of security. In fact, "[o]n a grading scale of A through F, experts say, LinkedIn … would get, at best, a "D" for [its] security."[4]

21. LinkedIn failed to use a modern hashing and salting function, and therefore drastically exacerbated the consequences of a hacker bypassing its outer layer of security. In so doing, Defendant violated its Privacy Policy's promise to comply with industry standard protocols and technology for data security.

The Attack on LinkedIn's Database

22. Reports indicate that LinkedIn's servers were breached through a common hacking method known as an "SQL injection" attack. This hacking technique involves exploiting weaknesses existing in a company's website to penetrate deeper into back-end servers that

[3] In simplest terms for purposes of this Complaint, "hashing" refers to the process by which a password is inputted into a cryptographic hash function and converted into an unreadable, encrypted format.

[4] Lax Security at LinkedIn Is Laid Bare, http://www.nytimes.com/2012/06/11/technology/linkedin-breach-exposes-light-security-even-at-data-companies.html?_r=1&pagewanted=all (last visited November 26, 2012).

contain databases of sensitive user information.

23. A failure by LinkedIn to adequately protect its website against SQL injection attacks—in conjunction with improperly securing its users' PII—demonstrates that it employed a troubling lack of industry standard security measures and protocols.

24. In fact, the Federal Trade Commission ("FTC") has filed complaints against corporations claiming to secure customer data while remaining vulnerable to SQL injection attacks.[5] For example, the FTC filed a complaint in 2003 against the "Guess?" clothing company. The complaint alleges that despite a posted policy ensuring reasonable Internet security measures, "Guess?" stored customers' PII in an unencrypted database concomitantly with poor website security. The FTC argued that these practices constituted unfair or deceptive practices affecting commerce in violation of federal law.

25. Moreover, the National Institute of Standards and Technology provides basic network security checklists that enumerate steps to avoid SQL injection vulnerabilities.[6] The failure of a large company tasked with protecting millions of users' PII, such as LinkedIn, to act pursuant to these basic security checklists would further belie its assertion that it employed industry standard protocols and technology to secure its customers' PII.

26. Had LinkedIn used proper encryption methods, and a hacker was able to penetrate LinkedIn's network, he would be limited in his ability to inflict harm. For example, though a hacker still might be able to cause temporary internal havoc in the operation of the website, or "vandalize" the appearance of webpages by altering their code, he would not be able to access user databases. Moreover, if LinkedIn used appropriate encryption methods—but still failed to secure its database—the stolen PII would be useless, as it would be indecipherable.

27. On June 6, 2012, a list of approximately 6.5 million hashed passwords retrieved

---

[5] *In the Matter of Guess?, Inc. and Guess.com Inc.*, (Case No. C-4091) (FTC, July 30, 2003) (available at http://www.ftc.gov/os/2003/08/guesscomp.pdf).

[6] National Checklist Program Repository, http://checklists.nist.gov (last visited November 26, 2012).

from LinkedIn's database was publicly posted online by hackers. Because the passwords were only hashed with a weak hashing function (and not salted), individuals were able to quickly decipher a large contingency of the posted passwords in a matter of hours. It quickly became apparent that the passwords belonged to LinkedIn users.

28. The widespread exposure of LinkedIn users' passwords is deeply troubling. While on its face "a compromised LinkedIn account — where people rarely store more than their résumé — would not appear to have broad consequences . . . *hackers know full well that people tend to use the same password across multiple sites and will test those passwords on Web mail, bank, corporate or brokerage firm accounts, where precious personal and financial data is free for the taking.*"[7]

29. Moreover, while only LinkedIn users' passwords were confirmed to be published online, the information taken from LinkedIn's databases was not limited to just passwords, but instead, on information and belief, also included the additional login credential of LinkedIn users' e-mail addresses.[8] While the publication of the passwords alerted LinkedIn and the public to the breach, the complete set of passwords and e-mail addresses were and are in the possession of the individuals who hacked LinkedIn's database, and such data could easily and quickly be shared with or sold to others (which may have already occurred). Simply stated, the publication of the passwords is only one facet of the harm inflicted by LinkedIn's insufficient security measures.

30. Only after third party observers publicly announced the origin of the password list did LinkedIn become aware that its security had even been breached and that confidential information had been removed. Initially, LinkedIn publicly responded by stating, "[o]ur security

[7] Lax Security at LinkedIn Is Laid Bare, http://www.nytimes.com/2012/06/11/technology/linkedin-breach-exposes-light-security-even-at-data-companies.html?_r=1&pagewanted=all (last visited November 26, 2012).

[8] *Id*. ("In its blog post, LinkedIn noted that the user names associated with those passwords had not been posted online, but security experts say that is probably because whoever breached its systems simply kept those for themselves.")

team continues to investigate this morning's reports of stolen passwords. At this time, we're still unable to confirm that any security breach has occurred."[9]

31. However, on June 9, 2012, LinkedIn admitted that it was not handling user data in accordance with best practices. LinkedIn stated that "one of our major initiatives was the transition from a password database system that hashed passwords, *i.e*. provided one layer of encoding, to a system that both hashed and salted the passwords, *i.e*. provided an extra layer of protection that is a widely recognized best practice within the industry. That transition was completed prior to news of the password theft breaking on Wednesday. We continue to execute on our security roadmap, and we'll be releasing additional enhancements to better protect our members."[10] But these actions were too little too late—LinkedIn's transition to industry standard data protection practices clearly occurred *after* its servers were breached, as the passwords publicly posted were, by its own admission, only hashed.

32. The fact that LinkedIn did not recognize its databases had been compromised until it was informed through public channels provides further evidence that the company did not adhere to industry standards. Specifically, LinkedIn did not implement, or it poorly implemented, an intrusion detection system to properly identify and quickly respond to attacks on its servers.

33. As such, LinkedIn's failure to protect Plaintiffs' and the Class members' PII with industry standard protocols and technology significantly contributed to the hacker's ability to gain access to LinkedIn's network, and to ultimately decipher and disclose Plaintiff Wright's and the Subclass members' PII to the public.

LinkedIn's Business Model

34. LinkedIn offers products and services in the form of online applications to be

---

[9] Updating Your Password on LinkedIn and Other Account Security Best Practices, http://blog.linkedin.com/2012/06/06/updating-your-password-on-linkedin-and-other-account-security-best-practices/ (last visited November 26, 2012).

[10] An Update On Taking Steps To Protect Our Members, http://blog.linkedin.com/2012/06/09/an-update-on-taking-steps-to-protect-our-members/ (last visited November 26, 2012).

used in conjunction with online social networks.

35. LinkedIn's consumers pay for LinkedIn's products and services both with actual dollars and with their PII. Put another way, in addition to a more conventional subscription fee, users buy products and services by paying LinkedIn in the form of contact information (first name, last name, and an e-mail address). Put yet another way, LinkedIn users provide something valuable—access to their personal information—in exchange for LinkedIn's products and services, which include LinkedIn's promise to employ industry standard protocols and technology to safeguard their PII.

36. LinkedIn is able to generate earnings from users through the receipt of their PII. LinkedIn describes itself as a "unique social application-based advertising network." In other words, in addition to its subscription fees, LinkedIn makes money by selling targeted advertising space, similar to a newspaper or television program.

37. Thus, the promises contained in its Privacy Policy concerning the safeguarding of consumer data are vital to its business and to its consumers.

FACTS RELATING TO PLAINTIFF KATIE SZPYRKA

38. During the relevant time period, Plaintiff Katie Szpyrka was a registered account holder with LinkedIn. She registered for an account with LinkedIn in or around late 2010.

39. Beyond simply being a registered user of LinkedIn, Plaintiff Szpyrka additionally paid a monthly fee to use LinkedIn's premium services. From approximately late 2010 to November 2011, she paid $24.95 per month, and from December 2011 to the present she has paid $26.95 per month.

40. In signing up to utilize LinkedIn, Plaintiff Szpyrka submitted her first name, last name, e-mail address, and a unique password to Defendant.

41. In creating an account with Defendant, Plaintiff Szpyrka agreed to and relied upon LinkedIn's User Agreement and Privacy Policy, including the material term that "Personal information you provide will be secured in accordance with industry standard protocols and

technology."

42. The monthly fees, or a portion thereof, that Szpyrka paid to Defendant was used by Defendant to pay for the administrative costs of data management and security, and to otherwise comply with its promise to use "industry standard protocols and technology" to protect the Class members' PII.

43. Had Plaintiff Szpyrka known of Defendant's substandard security procedures and methods of protecting and storing her PII, she would have paid less, or not paid at all, for Defendant's services. Plaintiff Szpyrka did not receive the benefit of the bargain in that the services provided were worth less than she paid for them, and that she paid more than she otherwise would have based upon Defendant's User Agreement and Privacy Policy.

44. Moreover, had Plaintiff Szpyrka known of Defendant's substandard security procedures and methods of protecting and storing her PII, she would not have provided her personal and confidential information in exchange for access to Defendant's services. Plaintiff Szpyrka did not receive the benefit of the bargain in that the services provided were not commensurate with the value of the personal information she provided in exchange, and Plaintiff provided more information than she otherwise would have based upon Defendant's User Agreement and Privacy Policy.

45. Plaintiff Szpyrka has suffered damages in the form of monies paid to Defendant for her premium LinkedIn membership.

FACTS RELATING TO PLAINTIFF KHALILA WRIGHT

46. During the relevant time period, Plaintiff Khalila Wright was a registered account holder with LinkedIn. She registered for an account with LinkedIn in or around March 2010. In signing up to utilize LinkedIn, Plaintiff Wright submitted her first name, last name, e-mail address, and a unique password to Defendant.

47. Beyond simply being a registered user of LinkedIn, Plaintiff Wright additionally paid a monthly fee of $99.95 to use LinkedIn's upgraded, premium services.

48. In creating an account with Defendant, Plaintiff Wright agreed to and relied upon LinkedIn's User Agreement and Privacy Policy, including the material term that "Personal information you provide will be secured in accordance with industry standard protocols and technology."

49. On or about June 7, 2012, Plaintiff Wright received an e-mail from Defendant informing her that her LinkedIn account and password were compromised. Additionally, Plaintiff Wright's password was publically posted on the Internet on June 6, 2012.

50. The monthly fees, or a portion thereof, that Wright paid to Defendant was used by Defendant to pay for the administrative costs of data management and security, and to otherwise comply with its promise to use "industry standard protocols and technology" to protect the Class members' PII.

51. Had Plaintiff Wright known of Defendant's substandard security procedures and methods of protecting and storing her PII, she would have paid less, or not paid at all, for Defendant's services. Plaintiff Wright did not receive the benefit of the bargain in that the services provided were worth less than she paid for them, and that she paid more than she otherwise would have based upon Defendant's User Agreement and Privacy Policy.

52. Moreover, had Plaintiff Wright known of Defendant's substandard security procedures and methods of protecting and storing her PII, she would not have provided her personal and confidential information in exchange for access to Defendant's services. Plaintiff Wright did not receive the benefit of the bargain in that the services provided were not commensurate with the value of the personal information she provided in exchange, and Plaintiff provided more information than she otherwise would have based upon Defendant's User Agreement and Privacy Policy.

53. Plaintiff Wright has suffered damages in (i) the form of monies paid to Defendant for her premium LinkedIn membership, and (ii) in the value of her personal data and lost property in the form of her breached and compromised PII.

CLASS ALLEGATIONS

54. Plaintiffs Szpyrka and Wright, respectively, bring this action pursuant to Fed. R. Civ. P. 23(b)(2) and (3) on behalf of themselves and a Class of similarly situated individuals, defined as:

> **Premium Account Class:** All individuals and entities in the United States who paid a monthly fee to LinkedIn for a premium account prior to June 7, 2012.

Additionally, Plaintiff Wright brings this action pursuant to Fed. R. Civ. P. 23(b)(2) and (3) on behalf of herself and a Subclass of similarly situated individuals, defined as:

> **Data Breach Subclass:** All Premium Account Class members whose personal information was compromised as a result of the data breach that occurred on or around June 6, 2012.

Excluded from the Premium Account Class ("Class") and Data Breach Subclass ("Subclass") are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and their current or former employees, officers and directors; (3) counsel for Plaintiffs and Defendant; (4) persons who properly execute and file a timely request for exclusion from the class; (5) the legal representatives, successors or assigns of any such excluded persons; (6) all persons who have previously had claims similar to those alleged herein finally adjudicated or who have released their claims against Defendant; and (7) any individual who contributed to the unauthorized access of Defendant's database.

55. **Numerosity**: The exact number of the members of the Class and Subclass is unknown to Plaintiffs at this time, but on information and belief, there are hundreds of thousands of persons in the Class and Subclass, making joinder of each individual member impracticable. Ultimately, members of the Class and Subclass will be easily identified through Defendant's records.

56. **Typicality**: Plaintiffs' claims are typical of the claims of all the other members of the Class and Subclass. Plaintiffs and the members of the Class and Subclass sustained substantially similar damages as a result of Defendant's uniform wrongful conduct, based upon

the same transactions that were made uniformly with Plaintiffs and the public.

57. **Adequate Representation**: Plaintiffs will fairly and adequately represent and protect the interests of the other members of the Class and Subclass. Plaintiffs have retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Class and Subclass, and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Class and Subclass.

58. **Superiority**: This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy because joinder of all parties is impracticable. The damages suffered by the individual members of the Class and Subclass will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Class and Subclass to obtain effective relief from Defendant's misconduct. Even if members of the Class and Subclass could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court. Economies of time, effort and expense will be fostered and uniformity of decisions ensured.

59. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class and Subclass, and those questions predominate over any questions that may affect individual members of the Class and Subclass. Common questions for the Class and Subclass include but are not limited to the following:

(a) whether LinkedIn failed to protect users' PII with industry standard

protocols and technology;

(b) whether LinkedIn's conduct described herein violates California's Unfair Competition Law (Cal. Bus. & Prof. Code §§ 17200, *et seq*.);

(c) whether LinkedIn's conduct described herein constitutes a breach of contract;

(d) whether LinkedIn's conduct described herein constitutes breach of the implied covenants of good faith and fair dealing;

(e) whether LinkedIn's conduct described herein constitutes breach of implied contracts;

(f) whether LinkedIn's conduct described herein was negligent and/or grossly negligent;

(g) whether LinkedIn's conduct described herein constitutes negligence *per se*; and

(h) whether LinkedIn has been unjustly enriched as a result of its conduct described herein.

60. **Policies Generally Applicable to the Class and Subclass**: LinkedIn has acted and failed to act on grounds generally applicable to Plaintiffs and the other members of the Class and Subclass, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class and Subclass.

61. Plaintiffs reserve the right to revise the definitions of the Class and Subclass based on further investigation, including facts learned in discovery.

FIRST CAUSE OF ACTION
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, *et seq*.
(On Behalf of Plaintiffs and the Class)

62. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

63. California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, *et seq*., protects both consumers and competitors by promoting fair competition in commercial

markets for goods and services.

64. The UCL prohibits any unlawful, unfair, or fraudulent business act or practice. A business practice need only meet one of the three criteria to be considered unfair competition. An unlawful business practice is anything that can properly be called a business practice and that at the same time is forbidden by law.

65. As described herein, Defendant's knowing and willful failure to safeguard and secure its users' sensitive PII violates the UCL.

66. Commonly accepted and widely practiced industry standards provide that sensitive PII stored in a commercial database should be not be accessible to extraction and simple decryption, and commercially reasonable methods to prevent such access are widely known throughout the security industry.

67. LinkedIn willfully and knowingly failed to expend the resources necessary to protect the sensitive data entrusted to it by Plaintiffs and the Class in clear contradiction of accepted industry standards for database security and its own Privacy Policy and User Agreement. In creating the perception that it followed industry standard protocols for database protection, and explicitly stating as much, LinkedIn gained an unfair advantage over its competitors.

68. Additionally, LinkedIn was likely to deceive consumers by providing in its Privacy Policy that its users' PII would be "protected with industry standard protocols and technology."

69. By failing to maintain its users' PII in a properly encrypted database, LinkedIn failed to use commercially reasonable safeguards to protect its users' PII. Storing sensitive PII in simple hashed values is not commercially reasonable and does not comport with industry standard protocols and technology, as promised.

70. By failing to employ industry standard protocols and technology to safeguard its users' personal data, LinkedIn violated its own written Privacy Policy and acted unfairly.

71. LinkedIn's representations regarding its security procedures were likely to mislead the public because they were authoritative descriptions made in the contracts between LinkedIn and its users. Because PII privacy and security is likely to, and does, affect consumers' willingness to use and pay for a service, LinkedIn's representations were material.

72. Defendant has violated the "unfair" prong of the UCL because it knowingly failed to employ industry standard protocols and technology for data protection, causing the widespread exposure of millions of consumers' PII. More specifically, LinkedIn's failure to protect Plaintiffs' and the Class members' PII with industry standard protocols and technology significantly contributed to the hacker's ability to gain access to LinkedIn's network, and to ultimately decipher and disclose Plaintiff Wright's and the Subclass members' PII to the public, as well as carry out other nefarious acts through the distribution and sale of the relevant email addresses and passwords. As a direct and proximate result of Defendant's unfair conduct, Plaintiffs and the Class have been injured in the form of monies paid to Defendant for monthly membership fees.

73. Defendant engaged in conduct, the utility of which is outweighed by the gravity of consequences to Plaintiffs and members of the Class. More specifically, Defendant engaged in unfair conduct where it failed to employ industry standard protocols and technology for data protection—despite its representations to the contrary—which ultimately lead to the exposure of millions of individuals', including Plaintiff Wright's and the Subclass members', sensitive PII. Additionally, Defendant's unfair conduct was substantially injurious to Plaintiffs and the members of the Class because Defendant knowingly collected monthly membership fees paid in part for LinkedIn promise to use industry standard protocols and technology to protect their PII, when in reality, it did not employ such practices.

74. Because Defendant maintained control over the database(s) containing Plaintiffs and the Class members' PII, Plaintiffs and the Class could not have reasonably avoided the injuries alleged herein.

75. Defendant's unfair or deceptive practices occurred primarily and substantially in California. Decisions concerning the retention and safeguarding of user information were made in California, LinkedIn maintains all or a substantial part of its computer systems containing user information in California, and the security breach of its computer systems took place primarily and substantially in California.

76. As a result of LinkedIn's conduct as alleged herein, Plaintiffs and the members of the Class have lost money in the form of monthly membership fees paid partially in exchange for LinkedIn promising to use industry standard protocols and technology to protect their PII. Additionally, Plaintiff Wright and the members of the Subclass have lost money and/or property in the form of the value of their personal data and have lost property in the form of their breached and compromised PII, which is of great value to LinkedIn, LinkedIn's advertisers, and malicious actors. Because LinkedIn failed to deliver on its bargained-and paid-for promises, Plaintiffs and the members of the Class have suffered economic damage.

77. Pursuant to Cal. Bus. & Prof. Code §§ 17203 and/or 17204, Plaintiffs seek an order permanently enjoining Defendant from continuing to engage in the unfair conduct described herein. Additionally, Plaintiffs seek an order requiring Defendant to: (1) immediately stop the unlawful practices described in this Complaint; (2) ensure that LinkedIn user data does not appear in Internet search engines; (3) ensure that LinkedIn employs commercially reasonable methods to safeguard its user data; (4) pay restitutionary disgorgement of all monies accruing to LinkedIn because of its unfair conduct described herein; and (5) pay attorney's fees, and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

SECOND CAUSE OF ACTION
Breach of Contract
(On Behalf of Plaintiffs and the Class)

78. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

79. In order to use its social networking applications, Defendant required that Plaintiffs and the members of the Class affirmatively assent to its User Agreement and Privacy

Policy (the "Agreement"). Plaintiffs and the Class assented to the Agreement by registering for, paying money for a premium account, and using LinkedIn's service.

80. The Agreement's provisions constitute a valid and enforceable contract between Plaintiffs and the members of the Class on the one hand, and Defendant on the other.

81. Under the terms of the Agreement, Plaintiffs and the members of the Class agreed to pay LinkedIn a monthly fee in exchange for certain of LinkedIn's products and services, and LinkedIn's promise to use "industry standard protocols and technology" to protect their PII.

82. The monthly fees, or a portion thereof, that Plaintiffs and the members of the Class paid to LinkedIn were used by LinkedIn to pay for the administrative costs of data management and security, and to otherwise comply with its promise to use industry standard protocols and technology to protect their PII.

83. As described herein, Defendant materially breached the terms of the Agreement by failing to use industry standard protocols and technology to protect Plaintiffs' and Class and members' PII as promised.

84. As a result of Defendant's misconduct and breach of the Agreement described herein, Plaintiffs and the members of the Class suffered injury in the form of monies paid to Defendant. Plaintiffs and the members of the Class did not receive the benefit of the bargain for which they contracted, and for which they paid monthly fees.

THIRD CAUSE OF ACTION
Restitution/Unjust Enrichment
(*in the alternative to Count II*)
(On Behalf of Plaintiffs and the Class)

85. Plaintiffs incorporate the foregoing allegations as if fully set forth herein, excluding paragraphs 78–84 and 92–98.

86. If the Court finds Plaintiffs' and the Class members' contracts with Defendant invalid or unenforceable, Plaintiffs and the Class members will have no valid contractual relationship with Defendant.

87. Plaintiffs and Class members conferred a monetary benefit on Defendant. That is,

Defendant received and retained money belonging to Plaintiffs and the Class in the form of monthly membership fees paid to Defendant.

88. Defendant appreciates or has knowledge of such benefit.

89. The monthly premiums that Plaintiffs and the Class paid to Defendant were used, in part, to pay for the administrative costs of data management and security of their PII.

90. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and the members of the Class, because Defendant failed to implement the data management and security measures that are mandated by industry standards.

91. As a result of Defendant's conduct, Plaintiffs and the members of the Class have suffered actual damages in the form of the monthly fees paid to Defendant in exchange for certain of its products and services, including the portion thereof used by Defendant for the administrative costs of data management and security, and to otherwise comply with its promise to use "industry standard protocols and technology" to protect the Plaintiffs and the Class members' PII.

FOURTH CAUSE OF ACTION
Breach of Contract
(On Behalf of Plaintiff Wright and the Subclass)

92. Plaintiff Wright incorporates the foregoing allegations as if fully set forth herein.

93. In order to use its social networking applications, Defendant required that Plaintiff Wright and the members of the Subclass affirmatively assent to the Agreement. Plaintiff Wright and the Subclass assented to the Agreement by registering for, paying money for a premium account, and using LinkedIn's service.

94. The Agreement's provisions constitute a valid and enforceable contract between Plaintiff Wright and the members of the Subclass on the one hand, and Defendant on the other.

95. Under the terms of the Agreement, Plaintiff Wright and the members of the Subclass agreed to pay LinkedIn a monthly fee in exchange for certain of LinkedIn's products and services, and LinkedIn's promise to use "industry standard protocols and technology" to

protect their PII.

96. The monthly fees, or a portion thereof, that Plaintiff Wright and the members of the Subclass paid to LinkedIn were used by LinkedIn to pay for the administrative costs of data management and security, and to otherwise comply with its promise to use industry standard protocols and technology to protect their PII.

97. As described herein, Defendant materially breached the terms of the Agreement by failing to use industry standard protocols and technology to protect Plaintiff Wright's and the Subclass members' PII as promised. LinkedIn's failure to protect Plaintiff Wright's and the Subclass members' PII with industry standard protocols and technology significantly contributed to the hacker's ability to gain access to LinkedIn's network, and to ultimately decipher and disclose Plaintiff Wright's and the Subclass members' PII to the public, as well as carry out other nefarious acts through the distribution and sale of the relevant email addresses and passwords.

98. As a result of Defendant's misconduct and breach of the Agreement described herein, Plaintiff Wright and the members of the Subclass suffered injury in (i) the form of monies paid to Defendant, and (ii) in the value of their personal data and lost property in the form of their breached and compromised PII, which is of great value to LinkedIn, LinkedIn's advertisers, and malicious actors. Plaintiff Wright and the members of the Subclass did not receive the benefit of the bargain for which they contracted, and for which they paid monthly fees.

FIFTH CAUSE OF ACTION
Restitution/Unjust Enrichment
(*in the alternative to Count IV*)
(On Behalf of Plaintiff Wright and the Subclass)

99. Plaintiff Wright incorporates the foregoing allegations as if fully set forth herein, excluding paragraphs 78–84 and 92–98.

100. If the Court finds Plaintiff Wright's and the Subclass members' contracts with Defendant invalid or unenforceable, Plaintiff Wright and the Subclass members will have no valid contractual relationship with Defendant.

101. Plaintiff Wright and the Subclass members conferred a monetary benefit on Defendant. That is, Defendant received and retained money belonging to Plaintiff Wright and the Subclass in the form of monthly membership fees paid to Defendant.

102. Defendant appreciates or has knowledge of such benefit.

103. The monthly premiums that Plaintiff Wright and the Subclass paid to Defendant were used, in part, to pay for the administrative costs of data management and security of their PII.

104. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff Wright and the members of the Subclass, because Defendant failed to implement the data management and security measures that are mandated by industry standards.

105. As a result of Defendant's conduct, Plaintiff Wright and the members of the Subclass have suffered actual damages in (i) the form of the monthly fees paid to Defendant in exchange for certain of its products and services, including the portion thereof used by Defendant for the administrative costs of data management and security, and to otherwise comply with its promise to use "industry standard protocols and technology" to protect the Plaintiff Wright's and the Subclass members' PII, and (ii) in the value of their personal data and lost property in the form of their breached and compromised PII, which is of great value to LinkedIn, LinkedIn's advertisers, and malicious actors.

SIXTH CAUSE OF ACTION
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiffs the Class)

106. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

107. In order to use Defendant's social networking site, Plaintiffs and the members of the Class affirmatively assented to Defendant's User Agreement and Privacy Policy.

108. The Agreement's provisions—including LinkedIn's promise to use "industry standard protocols and technology" to protect Plaintiffs' and the Class members' PII—constitute

a valid and enforceable contract between Plaintiffs and the members of the Class on the one hand, and Defendant on the other.

109. Implicit in the Agreement were contract provisions that prevented Defendant from engaging in conduct that frustrated or injured Plaintiffs' and Class members' rights to receive the benefits of the Agreement.

110. Defendant's obligation to use "industry standard protocols and technology" to safeguard and secure Plaintiffs' and the Class members' sensitive PII was a material term of the Agreement.

111. Furthermore, implicit in the terms of the Agreement was Defendant's obligation to comply with Cal. Bus. & Prof. Code §§ 17200, *et seq*.

112. Defendant breached the implied covenant of good faith and fair dealing where it knowingly failed to safeguard and secure sensitive PII from unauthorized access and theft and further where it failed to fully comply with the proscriptions of applicable statutory law. In so doing, LinkedIn acted consciously and deliberately.

113. Defendant's misconduct and breach of the implied covenant of good faith and fair dealing as described herein resulted in injury to Plaintiffs and the members of the Class in the form of the monthly fees paid in exchange for certain of Defendant's products and services, including the portion thereof used by Defendant for the administrative costs of data management and security, and to otherwise comply with its promise to use "industry standard protocols and technology" to protect the Plaintiffs and the Class members' PII.

SEVENTH CAUSE OF ACTION
Breach of Implied Contracts
(On Behalf of Plaintiffs and the Class)

114. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

115. In order to use Defendant's social-networking site, Plaintiffs and Class members transmitted sensitive PII to Defendant, including their e-mail addresses and corresponding passwords, and paid monthly fees in order to use Defendant's services.

116. By providing that sensitive PII, and upon Defendant's acceptance of such information and monthly fees, Plaintiffs and Class members, on the one hand, and Defendant, on the other hand, entered into implied contracts whereby Defendant was obligated to take commercially reasonable steps to secure and safeguard Plaintiffs' and Class members' PII.

117. Without such implied contracts, Plaintiffs and the Class members would not have provided their PII nor would they have paid monthly fees to Defendant.

118. By failing to properly secure Plaintiffs' and the Class members' PII, Defendant breached its implied contracts with Plaintiffs and the members of the Class.

119. Defendant's breaches and other misconduct described herein resulted in injury to Plaintiffs and Class members in the form of the monthly fees paid in exchange for certain of Defendant's products and services, including the portion thereof used by Defendant for the administrative costs of data management and security, and to otherwise comply with its promise to use "industry standard protocols and technology" to protect the Plaintiffs and the Class members' PII.

120. Additionally, Plaintiff Wright and the members of the Subclass have lost money and/or property in the form of the value of their personal data and have lost property in the form of their breached and compromised PII, which is of great value to LinkedIn, LinkedIn's advertisers, and malicious actors.

EIGHTH CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

121. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

122. In order to use Defendant's social-networking site, Plaintiffs and the Class members transmitted sensitive PII to Defendant, including their e-mail addresses and corresponding passwords, and paid monthly fees in order to use Defendant's services.

123. By agreeing to accept Plaintiffs' and the Class members' sensitive PII and the monthly fees paid to Defendant in order to use its services, Defendant assumed a duty, which

required it to exercise reasonable care to secure and safeguard that information and to utilize industry standard protocols and technology to do so.

124. Defendant failed to properly encrypt Plaintiffs' and the Class members' passwords in line with industry standards and best practices, thereby breaching its duties to Plaintiffs and the members of the Class.

125. By failing to take proper security measures to protect Plaintiffs' and the Class members' sensitive PII as described herein, Defendant acted with gross negligence and departed from all reasonable standards of care.

126. As a direct and proximate result of Defendant's failure to exercise reasonable care and use commercially reasonable security measures to protect the Plaintiffs' and the Class members' PII, its databases were accessed (*i.e.*, "hacked") without authorization, Plaintiff Wright's and the Subclass members' sensitive PII was compromised, and their information exposed—without authorization—to the public and other nefarious purposes. Had Defendant used "industry standard protocols and technology" to protect the Plaintiffs and the Class members' PII, it would have been drastically more difficult to decipher Plaintiff Wright's and the Subclass members' passwords. As such, Defendant's conduct contributed significantly to the exposure and loss of their PII.

127. A security breach and unauthorized access to Plaintiff Wright's and the Subclass members' PII was reasonably foreseeable by Defendant, particularly in light of the fact that protections necessary to secure and safeguard databases were well-known within the industry and had been successfully used to protect sensitive PII for years prior to this breach.

128. Data breaches involving the loss of PII have increased significantly over the past several years. As such, public policy strongly favors the use of industry standing protocols and technology to protect PII because the ramifications of data breaches can be substantial and can lead to actual damages including, but not limited to, economic damages, actual identity theft, and loss of privacy.

129. Neither Plaintiffs nor the other members of the Class contributed to the security breach or insufficient security described herein.

130. As a direct and proximate result of Defendant's misconduct described herein, Plaintiffs and the members of the Class were injured because (i) their PII was not properly secured and was thus subject to public disclosure without consent, (ii) they were deprived the benefit of the services for which they paid in the form of monthly fees, including the portion of which was used by Defendant for the administrative costs of data management and security, and to otherwise comply with its promise to use "industry standard protocols and technology" to protect the Plaintiffs and the Class members' PII, and (iii) they did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of their PII, which has ascertainable value to be proven at trial.

NINTH CAUSE OF ACTION
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

131. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

132. Defendant's violations of Cal. Bus. & Prof. Code §§ 17200, *et seq.* resulted in injury to Plaintiffs and the members of the Class.

133. The harm Defendant caused to Plaintiffs and the Class are injuries that result from the type of occurrences the statute was designed to prevent.

134. Plaintiffs and the members of the Class are the type of persons for whose protection the statute was adopted.

135. The harm caused to Plaintiffs and the members of the Class was reasonably foreseeable as a result of LinkedIn's breach of its duties, as the consequences of lax information security practices are particularly well-known within the social networking and data management industry.

136. Defendant's violations of the foregoing statute as described herein resulted in injury to Plaintiffs and the members of the Class. Plaintiffs and the members of the Class did not

receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of their PII that has ascertainable value to be proven at trial and the monthly fees paid in exchange for certain of Defendant's products and services, including the portion thereof used by Defendant for the administrative costs of data management and security, and to otherwise comply with its promise to use "industry standard protocols and technology" to protect the Plaintiffs and the Class members' PII.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Szpyrka and Wright, individually and on behalf of the Class and Subclass, pray for the following relief:

A. Certify this case as a class action on behalf of the Class and Subclass defined above, appoint Katie Szpyrka and Khalilah Wright as Class representatives, appoint Khalilah Wright as the Subclass Representative and appoint their counsel as Class counsel;

B. Declare that Defendant's actions, as described herein, violates California's Unfair Competition Law (Cal. Bus. & Prof. Code §§ 17200, *et seq.*), and constitutes breach of contract, breach of the implied covenant of good faith and fair dealing, breach of implied contract, negligence, and negligence *per se*;

C. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and the members of the Class and Subclass, including, *inter alia*: (i) an order prohibiting Defendant from engaging in the wrongful and unlawful acts described herein; (ii) ensuring that Defendant's user data does not appear in Internet search engines; and (iii) requiring Defendant to protect all data collected through the course of its business in accordance with industry standards;

D. Award appropriate restitution and/or damages to Plaintiffs and the members of the Class and Subclass in an amount to be determined at trial;

E. Award Plaintiffs and the Class and Subclass their reasonable litigation expenses and attorneys' fees;

F. Award Plaintiffs and the Class and Subclass pre- and post-judgment interest, to the extent allowable; and

G. Award such other and further relief as equity and justice may require

JURY TRIAL

Plaintiffs demand a trial by jury for all issues so triable.

Respectfully submitted,

Dated: November 26, 2012

KATIE SZPYRKA and KHALILAH WRIGHT, individually and on behalf of all others similarly situated,

By: /s/ Ari J. Scharg
One of Plaintiffs' Attorneys

SEAN P. REIS (SBN 184044)
(sreis@edelson.com)
EDELSON MCGUIRE, LLP
30021 Tomas Street, Suite 300
Rancho Santa Margarita, California 92688
Tel: (949) 459-2124

JAY EDELSON (Admitted *Pro Hac Vice*)*
(jedelson@edelson.com)
RAFEY S. BALABANIAN (Admitted *Pro Hac Vice*)
(rbalabanian@edelson.com)
ARI J. SCHARG (Admitted *Pro Hac Vice*)
(ascharg@edelson.com)
CHRISTOPHER L. DORE (Admitted *Pro Hac Vice*)
(cdore@edelson.com)
EDELSON MCGUIRE, LLC
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Tel: (312) 589-6370
*Interim Lead Counsel for Plaintiffs and the Putative Class and Subclass

LAURENCE D. KING (SBN 206423)**
(lking@kaplanfox.com)
LINDA M. FONG (SBN 124232)
(lfong@kaplanfox.com)
KAPLAN FOX & KILSHEIMER LLP
350 Sansome Street, Suite 400
San Francisco, CA 94104
Tel: (415) 772-4700
**Liaison Counsel for Plaintiffs and the Putative Class and Subclass

Additional Counsel for Plaintiffs and the Putative Class and Subclass:

JOSEPH J. SIPRUT
(jsiprut@siprut.com)
SIPRUT PC
122 South Michigan Avenue, Suite 1850
Chicago, Illinois 60603
Tel: (312) 588-1440

DAVID C. PARISI
(dcparisi@parisihavens.com)
PARISI & HAVENS LLP
15233 Valleyheart Drive
Sherman Oaks, California 91403
Tel: (818) 990-1299

DAN MAROVITCH
(dmarovitch@marovitchlaw.com)
MAROVITCH LAW FIRM, LLC
233 South Wacker Drive, 84th Floor
Chicago, Illinois 60606
Tel: (312) 533-1605

CERTIFICATE OF SERVICE

I, Ari J. Scharg, an attorney, certify that on November 26, 2012, I served the above and foregoing ***First Amended Consolidated Class Action Complaint*** by causing true and accurate copies of such paper to be filed and transmitted to all counsel of record via the Court's CM/ECF electronic filing system.

/s/ Ari J. Scharg